

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Special Agent Kyle Bishop, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Agriculture - Office of Inspector General (“USDA-OIG”). As such, I am an “investigative or law enforcement officer” within the meaning of 18 U.S.C. § 2510(7) in that I am an officer of the United States who is empowered by law to conduct investigations and to make arrests for federal felony offenses. I also am a “federal law enforcement officer” within the meaning of Rule 41 of the Federal Rules of Criminal Procedure.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and as a law enforcement officer, I am authorized to execute search warrants and arrest warrants issued under the authority of the United States. I am authorized to conduct and supervise investigations relating to the programs and operations of the USDA; to make arrests, execute warrants, and carry firearms as authorized by the Agriculture and Food Act of 1981 (P.L. 97-98); and to exercise all duties and responsibilities authorized by the Inspector General Act of 1978 or incident thereto, including the authority to obtain USDA records and information, to administer oaths, and to undertake other duties as necessary in support of the mission of the OIG.

3. I have over ten years of experience as a law enforcement officer. I am a graduate of the Criminal Investigator Training Program at the Federal Law Enforcement Training Center, the Rhode Island Police Academy, and the U.S. Coast Guard Maritime Law Enforcement Academy. I hold a bachelor’s degree in criminal justice and a master’s degree in education.

PURPOSE OF AFFIDAVIT

4. I am investigating Reynaldo Martinez (“MARTINEZ”) and his partner Yanaiza Rodriguez (“RODRIGUEZ”) for alleged violations of 18 U.S.C. § 1028A (Aggravated Identity Theft), 18 U.S.C. § 1343 (Wire Fraud), 7 U.S.C. § 2024(b) (Illegal Acquisition or Use of Supplemental Nutrition Assistance Program Benefits); 42 U.S.C. § 408(a)(7)(B) (Misuse of a Social Security Number); and 18 U.S.C. § 371 (Conspiracy) (collectively, “SUBJECT OFFENSES”) in relation to the fraudulent schemes occurring in Districts of Rhode Island and Massachusetts. I am conducting the investigation with other federal agents of the Social Security Administration - Office of Inspector General (“SSA-OIG”), U.S. Postal Inspection Service (“USPIS”), and Treasury Inspector General for Tax Administration (“TIGTA”) as well as the Rhode Island Office of Internal Audit (“OIA”), Rhode Island State Police, Warwick Police Department, West Warwick Police Department, and Foxborough Police Department.

5. This affidavit is made in support of an Application for a Search Warrant for the following place, persons, and vehicle:

- a. The residence of MARTINEZ and RODRIGUEZ at [REDACTED], [REDACTED], Rhode Island (“SUBJECT PREMISES”) and further described in Attachment A-1, for the items described in Attachment B;
- b. The person of MARTINEZ, year of birth 1992 (“SUBJECT PERSON 1”), and further described in Attachment A-2, for the items described in Attachment B.
- c. The person of RODRIGUEZ, year of birth 1993 (“SUBJECT PERSON 2”), and further described in Attachment A-3, for the items described in Attachment B.

- d. The vehicle operated by and leased to MARTINEZ, a grey 2024 Acura MDX sport utility vehicle (“SUBJECT VEHICLE”), and further described in Attachment A-4, for the items described in Attachment B.

6. As set forth below, I believe probable cause exists to show evidence, fruits, and instrumentalities of crimes committed by MARTINEZ and RODRIGUEZ (collectively, “SUBJECT PERSONS”) and other co-conspirators will be found at the SUBJECT PREMISES, on the SUBJECT PERSONS, and in the SUBJECT VEHICLE, including on the electronic devices such as cell phones and computers located in or on these particularly described locations.

7. This affidavit is based on my personal knowledge, my review of reports and records used herein, and information provided to me by other agents of the government including OIA Internal Audit Manager Brittney Badway, SSA-OIG Special Agent Robert Beard, and U.S. Postal Inspector Cory McManus. This affidavit is not intended to set forth all the information that I have learned during this investigation but includes only the information necessary to establish probable cause for the search warrants for the SUBJECT PREMISES, SUBJECT PERSONS, and SUBJECT VEHICLE.

Background Information on SNAP

8. The statements in this section are based on my training and personal experience investigating identity and other fraud, and on information provided to me by other investigators.

9. Congress enacted SNAP to “promote the general welfare, to safeguard the health and well-being of the nation’s population by raising levels of nutrition among low-income households.” 7 U.S.C. § 2011. This program enables low-income households to obtain a more nutritious diet by increasing their food purchasing power.

10. Under the program, eligible households receive food stamps in the form of credits to an electronic benefit card to buy food from retail food stores that participate in SNAP. Food stamp benefits are obligations of the United States and redeemable at face value by the Secretary through the facilities of the Treasury of the United States. 7 U.S.C. § 2024(d). USDA administers SNAP nationally. Individuals or families that are in need of SNAP benefits may apply for assistance through the Rhode Island Department of Human Services (“RI DHS”).

11. It is unlawful to knowingly use, transfer, acquire, alter, or possess SNAP benefits in any manner contrary to Title 7 of United States Code or the regulations issued by the USDA. Violations of the section are punishable by a fine of not more than \$250,000 or imprisonment for not more than twenty years. 7 U.S.C. § 2024(b).

12. The Secretary of Agriculture may subject to forfeiture and denial of property rights any nonfood items, moneys, negotiable instruments, securities, or other things of value that are furnished by any person in exchange for benefits, or anything of value obtained by use of an access device, in any manner contrary to this chapter or the regulations issued under this chapter. Any forfeiture and disposal of property forfeited under this subsection shall be conducted in accordance with procedures contained in regulations issued by the Secretary. 7 U.S.C. § 2024(e).

13. Rhode Island uses the Electronic Benefit Transfer (“EBT”) system for SNAP benefits. The EBT system uses plastic debit cards, which are automatically credited with the recipient’s appropriate amount of benefits during certain times of each month. In the State of Rhode Island, SNAP benefits are credited to recipient’s accounts on the first of every month. To access benefits, the recipient presents the card at an authorized retailer’s location. The card is swiped through an electronic terminal device (commonly and hereinafter referred to as an “EBT terminal”) which reads coded information on the card’s magnetic strip. The transaction amount is

deducted from the EBT card's balance and deposited into the retailer's account.

14. When making a purchase from an authorized vendor, an EBT card user swipes the card through the EBT terminal and enters a personal identification number ("PIN") via a PIN pad. The terminal communicates via a financial network through a processing switch with a central database, which maintains recipient account balance information. The central database verifies the amount of benefits available, authorizes the transaction and deducts the purchase amount from the recipient's available balance. The system also calculates cumulative SNAP sales for each retailer and authorizes electronic payments to the retailer's bank account.

15. Investigators have the ability to monitor the SNAP EBT transactions at a particular store by accessing the database of the financial institution that is contracted to implement the SNAP EBT program. Throughout this investigation, the financial institution contracted in Rhode Island for the SNAP EBT program was Fidelity National Information Services, Inc ("FIS") which is headquartered in Jacksonville, Florida. Rhode Island uses ebtEDGE, a database maintained by FIS, to administer SNAP benefits. FIS uses a data center located in Phoenix, Arizona to house the individual Rhode Island EBT cardholder transaction data, and the daily settlement payments made to retailers in Rhode Island. These financial institutions provide an electronic means of identifying the locations of retailers that were visited by the SNAP EBT participant. This monitoring allows the investigators to view the transaction by card number at the store as it is being processed for redemption. It also allows the investigators to see the dollar amount of the transaction.

16. Retailers must obtain a license from the USDA Food and Nutrition Service ("FNS") to accept food stamp benefits from eligible recipients as payment for authorized food purchases. Before receiving authorization to participate in SNAP, a retailer is provided with an application to participate in SNAP and a book of federal regulations regarding SNAP. As part of the application

filled out by a retailer seeking to participate in SNAP, the retailer is advised of the SNAP regulations, including those prohibiting the retailer from providing cash or ineligible items to recipients in exchange for the recipient's SNAP benefits.

17. FNS has designated what types of items are eligible for purchase using SNAP benefits and what types of items are ineligible for purchase using SNAP benefits. Typical eligible items include bread/cereal, dairy products, fruits, vegetables, meat, poultry, fish, etc. Typical ineligible items include gasoline, tobacco products, alcohol, paper products, cleaning products, etc.

18. In Rhode Island, SNAP benefits are administered to recipients by RI DHS in accordance with federal requirements. RI DHS is responsible for determining SNAP eligibility and authorizing benefits for low-income households (participants) in need. RI DHS is staffed by state employees who operate staff offices and facilitate online infrastructure.

19. To qualify for SNAP in Rhode Island, the applicant must be a resident of Rhode Island, meet the financial eligibility requirements, and be a United States citizen or an eligible non-citizen, such as Lawful Permanent Resident (LPR) who has earned, or can be credited with, 40 quarters of work. An applicant for SNAP benefits must also provide proof of their identity, i.e., the applicant must be the person who they claim to be. An applicant must also furnish a Social Security Number ("SSN") or provide proof that the applicant has applied for one.

20. An applicant for SNAP benefits must provide complete and accurate information both at the time of application and on an ongoing basis to properly assess initial and continued eligibility for benefits.

21. When a recipient submits an application requesting SNAP, RI DHS has 30 thirty days to determine eligibility. In some limited cases, if the application indicates that the applicant

meets any one of the enumerated “Expedited Guidelines”, the application will be processed within seven days.

22. If any one of these criteria are met, the household will meet expedited status, and an eligibility technician will contact the applicant within seven days of the application being submitted for an interview. Expedited benefit applicants receive maximum benefits for 1 month or prorated and 1 month. If the applicant completes the scheduled interview, the benefits will be approved for 12 months, if the applicant submits an interim report after 6 months.

23. If the eligibility technician is unable to contact the applicant, the individual will receive expedited benefits for the applying month but will not be approved for the 12-month period. Depending on the date the recipient submitted the application, they may receive a pro-rated benefit amount for the month in which they applied, plus the following month’s benefit amount. If the technician cannot reach the applicant, the technician will schedule an interview for a later date and forward the interview date to the applicant’s provided mailing address. If the applicant does not attend the interview, a correspondence titled Noticed of Missed Interview (“NOMI”) will be sent to the applicant’s mailing address, and the case will be closed.

24. The amount of SNAP benefits to which a program participant is entitled is electronically posted to the program participant’s account on a monthly basis. Applicant eligibility is determined by citizenship, income, and number of people living within a household. A SNAP household is defined as persons who live together and purchase and prepare meals together. In general, households with larger numbers of people or dependents will receive higher amounts of benefits. Monthly benefits for SNAP are primarily determined by household size (number of persons living in a household). In the continental United States during Fiscal Year 2025,

households typically receive between \$292 for a household of one person up to \$1,756 for a household of eight persons.

25. SNAP recipients can query the balance of funds on an EBT card by placing a telephone call to a toll-free number maintained by the financial institution providing the card. The telephone numbers calling the toll-free number are logged. In my experience reviewing SNAP-related records, it is common for an EBT card to be queried by one or two telephone numbers (typically the adults living in the household to whom the card was issued).

26. In Rhode Island, OIA performs the auditing function for the administration of state public assistance benefits, including the SNAP. The USDA-OIG has federal statutory oversight authority of the SNAP to investigate fraud, waste, and abuse.

PROBABLE CAUSE

Relevant Criminal History of Martinez

27. In 2012, the Boston, Massachusetts Police Department arrested MARTINEZ for the fraudulent use of a credit card and assault and battery.

28. In 2012, the Attleboro, Massachusetts Police Department arrested MARTINEZ for identity fraud (false impersonation), forging or uttering a forged credit card, larceny over \$250, credit card fraud over \$250, improperly receiving credit cards, unlawfully buying or selling credit cards, and receiving stolen property.

29. In 2013, the Providence, Rhode Island Police Department arrested MARTINEZ for the fraudulent use of credit cards.

30. In 2013, the Boston, Massachusetts Police Department arrested MARTINEZ for larceny over \$250, fraudulent use of a credit card, and assault and battery with injury.

31. In 2013, the Attleboro, Massachusetts Police Department arrested MARTINEZ for identity fraud (false impersonation), credit card fraud over \$250, use of a motor vehicle without authority, two counts of attempting to commit a card, and five counts of receiving stolen credit cards.

32. In 2014, the Mount Vernon City, New York Police Department arrested MARTINEZ for the possession of a forged instrument in the second degree.

33. In 2017, the Rhode Island State Police arrested MARTINEZ for obtaining money under false pretenses over \$1,500 and possessing false identification.

34. In 2017, the Seekonk, Massachusetts Police Department arrested MARTINEZ for larceny over \$250, forgery of a document, uttering false writings, forgery of a government document, credit card fraud over \$250, and identity fraud.

35. In 2017, the Warwick, Rhode Island Police Department arrested MARTINEZ for identity fraud.

36. During various times between May 2017 and December 2023, MARTINEZ was intermittently incarcerated in federal custody for a total of five years and eight months, as detailed further below.

37. In 2024, the Warwick, Rhode Island Police Department obtained an arrest warrant for MARTINEZ for passing counterfeit certificates or bills. Martinez was arrested on this warrant by the Pawtucket, Rhode Island Police Department on October 28, 2024.

Prior Federal Investigation

38. In June 2017, a federal grand jury in the District of Rhode Island returned a seven-count indictment of MARTINEZ for offenses related to access device fraud and aggravated

identity theft. The government alleged MARTINEZ orchestrated a scheme to use the stolen identity of numerous individuals to open retail store credit cards and lines of credit which he used to purchase tens of thousands of dollars' worth of goods in Rhode Island and Massachusetts.

39. In August 2017, a federal grand jury in the District of Rhode Island returned a nine-count superseding indictment charging MARTINEZ for offenses related to aggravated identity theft, access device fraud, bank fraud, and interstate transportation of stolen goods.

40. In November 2017, MARTINEZ pleaded guilty to the superseding indictment.

41. In his guilty plea, MARTINEZ admitted that beginning in March 2017, he used various sources, including internet websites, to obtain personal identification information of individuals, including their SSNs, dates of birth and addresses, after which he would have counterfeit identity documents bearing his photograph. MARTINEZ admitted that he used the counterfeit identity documents to secure credit to make purchases at various businesses including Sprint wireless phone locations, Kohl's Department Store, Sak's Fifth Avenue, Best Buy, Cardi's Furniture, Raymour & Flanigan Furniture, and Home Depot. MARTINEZ admitted that he used the stolen credit to make between \$40,000 and \$90,000 dollars in purchases, for which he had no intention of paying. The investigation also revealed that MARTINEZ used stolen identity information and counterfeit identity documents to access lines of credit to fraudulently obtain passenger vehicles from car dealerships.

42. In January 2018, U.S. District Court Judge John J. McConnell, Jr. sentenced MARTINEZ to 48 months incarceration, three years of supervised release, and restitution in the amount of \$38,126.62.

43. In August 2021, MARTINEZ violated the terms of his supervised release and was arrested.

44. In February 2022, MARTINEZ violated the terms of his supervised release and was arrested.

45. In February 2022, MARTINEZ appeared before U.S. District Court Magistrate Judge Lincoln D. Almond and admitted he violated the terms of his probation.

46. In April 2022, U.S. District Court Judge John J. McConnell, Jr. sentenced MARTINEZ to 24 months incarceration and four years of supervised release. MARTINEZ was released from federal custody on December 15, 2023.

47. Currently, MARTINEZ is on federal supervised release for his convictions related to aggravated identity theft, access device fraud, bank fraud, and interstate transportation of stolen goods.

48. MARTINEZ appeared before U.S. District Court Magistrate Judge Lincoln D. Almond on November 8, 2024, for a new supervised release violation based upon committing a new crime, as alleged by the Warwick Police Department investigation in 2024, referenced above.

SNAP Fraud Investigation

49. On or about September 20, 2024, the OIA received a report of a fraudulent incident from the RI DHS alleging a subject, later determined to be MARTINEZ, made false statements to fraudulently obtain SNAP benefits on September 18, 2024. The RI DHS reported a subject applied for SNAP benefits in person at a state office using one identity; the same subject applied for SNAP benefits in person at a different state office on the same day using another identity. The RI DHS determined the same subject used two additional identities on September 19, 2024, and September 20, 2024, to apply for SNAP benefits.

50. OIA investigators conducted a review of telephone numbers conducting telephone balance inquires on SNAP EBT cards associated with the four identities suspected as fraudulent by the RI DHS. The analysis resulted in the association of four specific telephone numbers being used to conduct telephone balance inquires on multiple SNAP accounts suspected to be fraudulent. The telephone numbers that conducted the telephone balance inquires include:

- a. [REDACTED] (“MARTINEZ PHONE 1”) which is listed as the telephone contact number for a SNAP account of “Reynaldo Martinez”;
- b. [REDACTED] (“RODRIGUEZ PHONE”) which is associated with RODRIGUEZ in the Accurant¹ database, listed as the telephone contact number on the SNAP account in name “Yanaiza Rodriguez,” as well as listed as a contact telephone number on publicly available social media post on the Facebook account of RODRIGUEZ advertising prepared food for sale in April 2024;
- c. [REDACTED] (“MARTINEZ PHONE 2”) associated with MARTINEZ in the Accurant database and an internet service subscription in his name for the SUBJECT PREMISES; and
- d. [REDACTED] (“MARTINEZ PHONE 3”) associated with MARTINEZ in the Accurant database.

51. Additional review of the applications involved in the fraudulent incident revealed the misuse of SSNs including the use of at least four SSNs assigned to deceased U.S. citizens, at least three living adult U.S. citizens, and at least one living juvenile U.S. citizen. Additionally, the

¹ The Accurant database is a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, et cetera based on public information sources.

SNAP applications used at least seven counterfeit identity documents, such as driver's licenses and a passport card, were used to support the applications.

52. Beginning in or about November 2023 and continuing to present, I believe that MARTINEZ and RODRIGUEZ fraudulently obtained at least 40 SNAP EBT cards using at least 24 identities through various fraudulent means including online SNAP applications containing false statements and in-person SNAP applications using counterfeit documents beginning in July 2024. MARTINEZ and RODRIGUEZ are associated with the fraudulent SNAP accounts with a loss amount of at least \$19,291.89 through a review of surveillance footage of EBT transactions at retail locations and analysis of telephone balance inquiries and telephone PIN establishment on the fraudulent SNAP accounts.

53. Additional SNAP benefits in the amount of \$8,292.25 were issued to the identity of MARTINEZ as a result of suspected false statements including, but not limited to underreporting income and/or household composition.

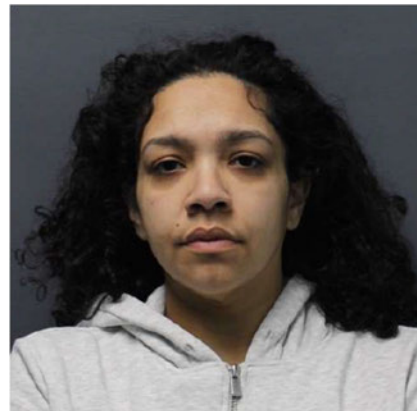
54. Internet protocol (IP) addresses associated with online activity logged in at least 14 of suspect SNAP accounts originated from an IP address assigned to RODRIGUEZ as recent as 2024, according to internet service provider (ISP) records. Additional activity from the IP address associated with RODRIGUEZ on at least six suspect SNAP accounts occurred in September 2023 and November 2023 when MARTINEZ was incarcerated, accord to ISP records.

55. An IP address associated with online activity logged in at least one of the suspect SNAP accounts originated from an IP address assigned to MARTINEZ at the SUBJECT PREMISES in June 2024, according to ISP records.

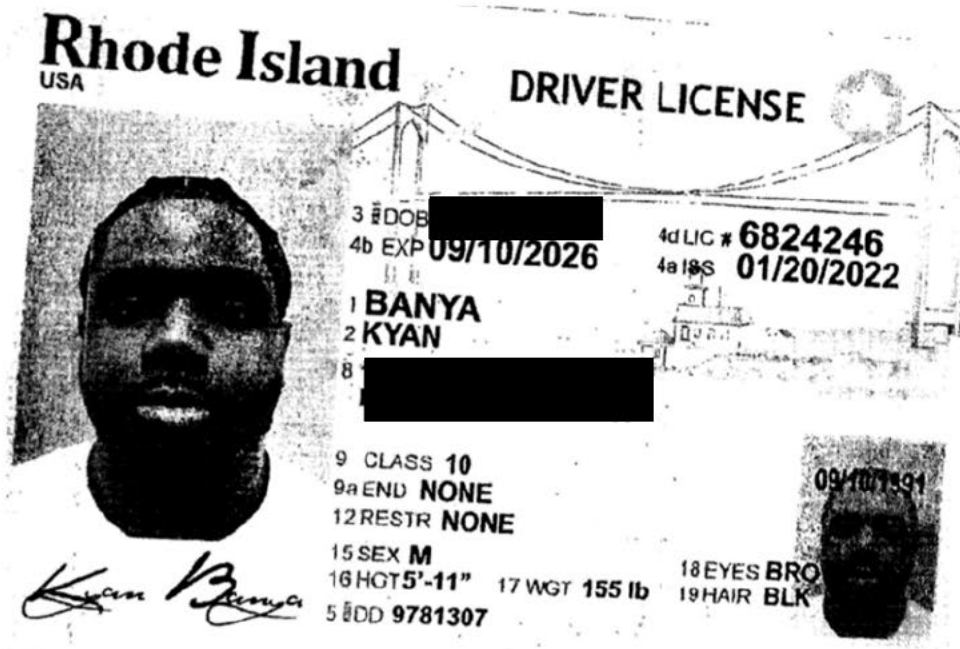
56. Images of MARTINEZ available to investigators include his Massachusetts driver's license photograph from 2012 (below left), an arrest booking photograph from 2017 (below center), and an arrest booking photograph from 2024 (below right).



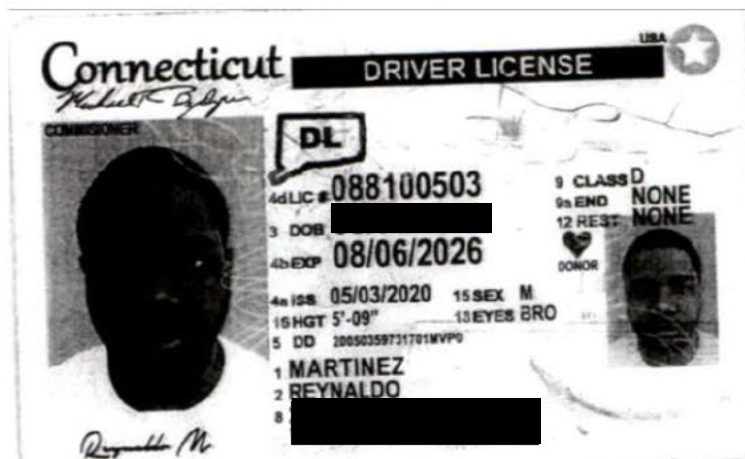
57. Images of RODRIGUEZ available to investigators include a license photograph from 2024 (below left) and an arrest booking photograph from 2024 (below right).



58. In April and July 2024, SNAP applications in the identity of K.B. were submitted to the state requesting the issuance of SNAP benefits. A counterfeit Rhode Island driver's license bearing an image of a person who I believe to be MARTINEZ was used to support the application. The counterfeit Rhode Island driver's license appears below.

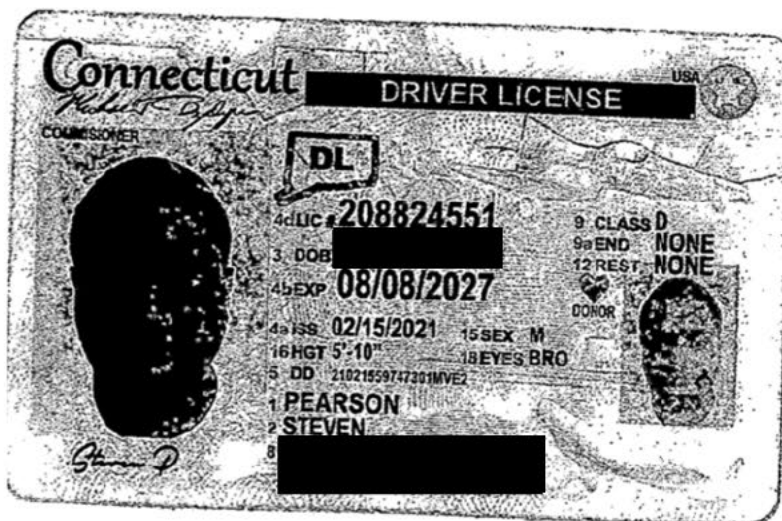


59. In July 2024, a SNAP application in the identity of MARTINEZ using a fraudulent date of birth and SSN was submitted to the state requesting the issuance of SNAP benefits. A counterfeit Connecticut driver's license bearing an image of a person who I believe to be MARTINEZ was used to support the application. The counterfeit Connecticut driver's license appears below.

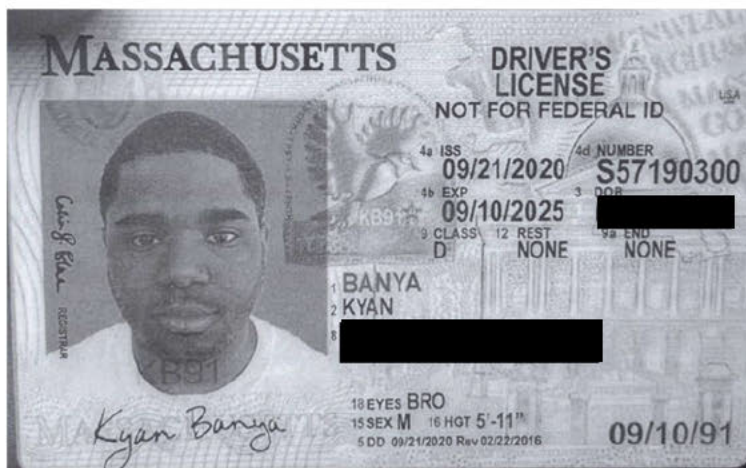


60. In August 2024, a SNAP application in the identity of S.P. was submitted to the state requesting the issuance of SNAP benefits. A counterfeit Connecticut driver's license bearing

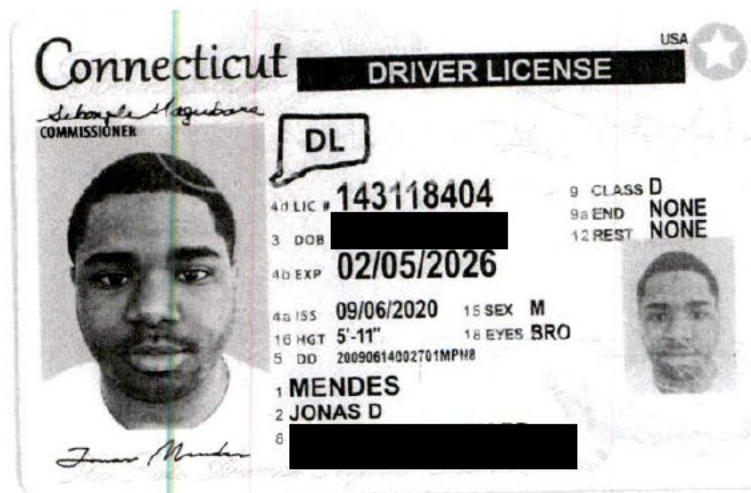
an image of a person who may be MARTINEZ was used to support the application. The counterfeit Connecticut driver's license appears below.



61. In October 2024, an additional SNAP application in the identity of K.B. was submitted to the state requesting the issuance of SNAP. In May 2024, a counterfeit Massachusetts driver's license bearing an image of a person who I believe to be MARTINEZ and using a previous residential address of MARTINEZ was used to obtain a line of credit to make a fraudulent the purchase of a vehicle in West Warwick, Rhode Island. The counterfeit Massachusetts driver's license appears below.



62. In October 2024, a SNAP application in the identity of J.M. was submitted to the state requesting the issuance of SNAP benefits. A counterfeit Connecticut driver's license bearing an image of a person who I believe to be MARTINEZ was used. The counterfeit Connecticut driver's license appears below.



Undercover SNAP Recipient Appointment

63. In January 2024, a SNAP application in the identity of J.J. was submitted to the state requesting the issuance of SNAP benefits. In August 2024, a subsequent SNAP application was submitted in this identity to continue benefits. The applicant indicated that he was homeless in the applications.

64. The MARTINEZ PHONE 1 conducted seven telephone balance inquiries on the SNAP EBT card issued to the identity of J.J. The MARTINEZ PHONE 1 also created the PIN for the SNAP account which is completed via telephone call.

65. Investigators arranged for a SNAP recipient appointment at a RI DHS office for the SNAP account holder to confirm information on the application which is a normal practice for SNAP administration. The appointment was arranged with the cooperation of RI DHS to appear

as a normal appointment. The undercover interaction was arranged by calling a telephone number associated with MARTINEZ and providing a date and time for “J.J.” to report a DHS office.

66. In an undercover capacity, a state investigator and I assumed the roles of RI DHS employees in an eligibility appointment room within the DHS office to await the arrival of the account holder for the SNAP account of J.J.

67. Investigators observed MARTINEZ arrive at the DHS office driving the SUBJECT VEHICLE and walk into the front entrance of the building. MARTINEZ approached the counter and identified himself as “J.J.,” provided a Social Security card in the name of J.J., and completed a “Homeless Declaration” form in the name “J.J.” MARTINEZ, under the name “J.J.,” received a ticket number 371 and sat in the waiting area for his appointment. An image of the form MARTINEZ signed, which was later seized as evidence, appears below.

Homeless Declaration

Date: 10 / 18 / 2024

I, Jason Johnson, declare that I do not have a permanent address and am presently homeless in the City of Providence.

I have presented verification that I will be using the following address to receive mail.

Address: 123 Holden St
Providence, RI

I have the following sources of income:

Signature: Jason Johnson

68. The state investigator assisting with the undercover operation summoned “J.J.” from the waiting room for his appointment to which MARTINEZ responded. MARTINEZ, who I recognized based on my review of his driver’s license and booking photographs, entered the eligibility appointment room. An image of MARTINEZ from the undercover interaction, which I documented with covert audio and video recordings, appears below.



69. MARTINEZ claimed to be J.J. during the eligibility interview. MARTINEZ handed me two counterfeit identity documents, a Rhode Island driver’s license in the identity of J.J. (bearing a photograph of MARTINEZ) and a Social Security card in the name of J.J. The Rhode

Island Division of Motor Vehicles confirmed the driver's license as counterfeit. Additionally, the Social Security Administration determined the Social Security card to be a real document altered to display the name of "J.J.," an unassigned SSN, and "03/23/2012" as the issue date. I photographed the counterfeit documents, which appear below, when I left the eligibility interview room to scan the documents which is a normal part of a legitimate SNAP application process.



70. During the eligibility interview, I observed MARTINEZ possess and manipulate a smart phone during the interaction. Based on my training and experience in similar investigations, individuals who are involved in obtaining fraudulent benefits frequently use telephones to query card balances to fraudulently use the benefits or provide the balance information to other individuals to whom they give or sell the cards. Smart phones can also be used to store and organize information on stolen identities.

71. During the eligibility interview, MARTINEZ made false statements including confirming a false date of birth and SSN and failing to disclosure income (from his multiple other fraudulent schemes). I returned the counterfeit documents to MARTINEZ and concluded the interview. MARTINEZ departed the building and drove away in the SUBJECT VEHICLE eventually traveling to Pawtucket, Rhode Island.

Video Surveillance of SNAP Transactions

72. On July 18, 2024, a SNAP transaction using the EBT card issued to the identity of S.R. occurred at Stop & Shop in Pawtucket, Rhode Island. The RODRIGUEZ PHONE conducted 19 telephone balance inquires on the EBT card issued to S.R., including approximately one hour before this transaction. The MARTINEZ PHONE 1 conducted three telephone balance inquires on the EBT card issued to S.R. Surveillance footage associated with the transaction shows subjects believed to be MARTINEZ and RODRIGUEZ.



73. On July 22, 2024, a SNAP transaction using the EBT card issued to the identity of S.R. occurred at Stop & Shop in Pawtucket, Rhode Island. Surveillance footage associated with the transaction shows a subject believed to be MARTINEZ.



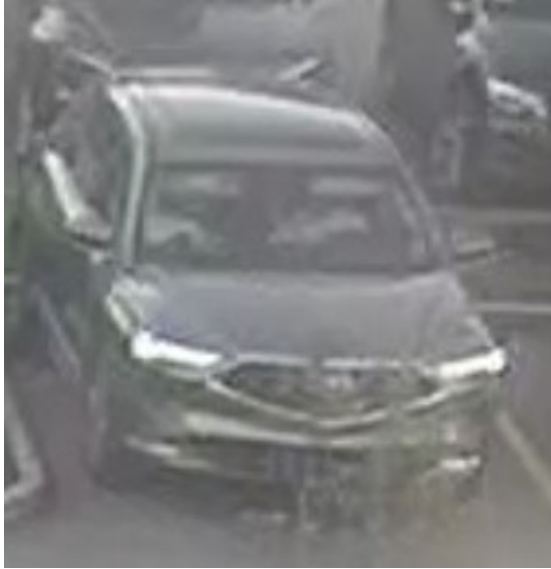
74. On August 16, 2024, a SNAP transaction using the EBT card issued to the identity of J.J. occurred at Stop & Shop in Pawtucket, Rhode Island. The MARTINEZ PHONE 1 conducted seven telephone balance inquires on the EBT card issued to J.J., including approximately an hour before this transaction. MARTINEZ previously provided me with counterfeit documents in the identity of J.J. during an undercover interaction in October 2024. Surveillance footage shows a subject believed to be MARTINEZ arriving in an Acura MDX believed to be the SUBJECT VEHICLE.



75. On August 24, 2024, a SNAP transaction using the EBT card issued to the identity of K.R. occurred at Price Rite in Providence, Rhode Island. The RODRIGUEZ PHONE conducted 13 telephone balance inquiries on the EBT card issued to K.R., including six times on the day of this transaction. The MARTINEZ PHONE 1 conducted two telephone balance inquiries on the EBT card issued to K.R. Surveillance footage associated with the transaction shows a subject believed to be RODRIGUEZ.



76. On September 5, 2024, a SNAP transaction using the EBT card issued to the identity of S.R. occurred at Market Basket in Warwick, Rhode Island. Surveillance footage associated with the transaction shows a subject believed to be RODRIGUEZ. Surveillance footage shows RODRIGUEZ arriving in an Acura MDX believed to be the SUBJECT VEHICLE.



77. On September 7, 2024, a SNAP transaction using the EBT card issued to the identity of S.P. occurred at Price Rite in Providence, Rhode Island. The MARTINEZ PHONE 1 conducted eight telephone balance inquiries on the EBT card issued to S.P., including three on the day before this transaction. The RODRIGUEZ PHONE conducted three telephone balance inquiries on the EBT card issued to S.P. Surveillance footage associated with the transaction shows a subject believed to be RODRIGUEZ.



78. On September 8, 2024, a SNAP transaction using the EBT card issued to the identity of S.P. occurred at Stop & Shop in Pawtucket, Rhode Island. Surveillance footage associated with the transaction shows a subject believed to be RODRIGUEZ. Surveillance footage shows RODRIGUEZ arriving in an Acura MDX believed to be the SUBJECT VEHICLE.



79. On September 20, 2024, a SNAP transaction using the EBT card issued to the identity of Q.M. occurred at Stop & Shop in Pawtucket, Rhode Island. Surveillance footage associated with the transaction shows subjects believed to be MARTINEZ and RODRIGUEZ. Surveillance footage shows MARTINEZ and RODRIGUEZ arriving in an Acura MDX believed to be the SUBJECT VEHICLE.



80. On September 26, 2024, a SNAP transaction using the EBT card issued to the identity of T.H. occurred at Walmart in Providence, Rhode Island. The MARTINEZ PHONE 1 conducted nine telephone balance inquires on the EBT card issued to T.H., including approximately ten minutes before this transaction and three additional queries on the day of the transaction. Surveillance footage from the transaction shows a subject believed to be MARTINEZ.

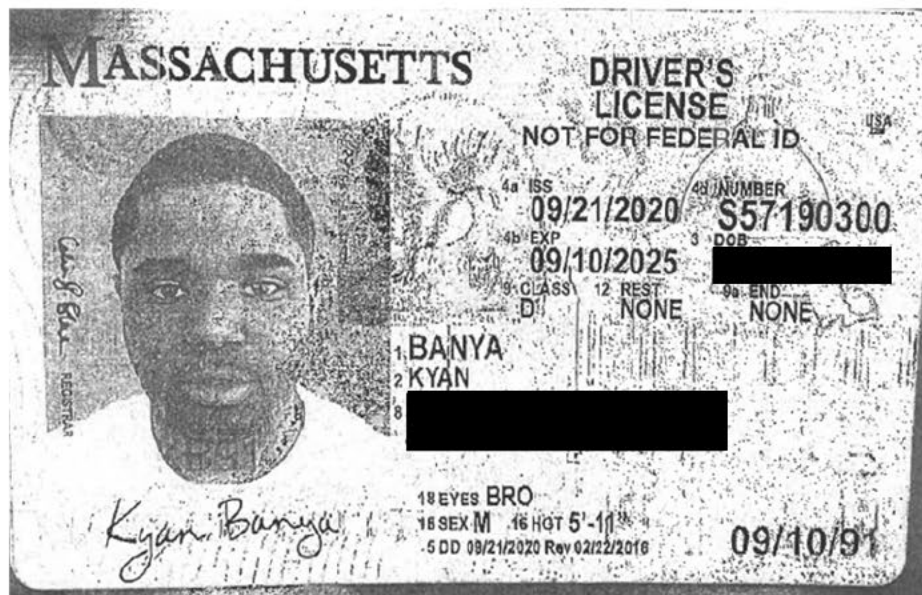


Vehicle Fraud Investigation

81. In February 2024, a subject, who I believe to be MARTINEZ, used a counterfeit Massachusetts driver's license in the identity of K.B. to obtain a 2024 Acura MDX sport utility vehicle (which is a different vehicle from the SUBJECT VEHICLE) from Speedcraft Acura car dealer in West Warwick, Rhode Island by obtaining a line of credit using stolen identity information and leaving the dealership with the vehicle. The fraud resulted in a loss up to

\$24,162.51 to Greenwood Credit Union which reported the fraud to the West Warwick Police Department in May 2024.

82. As detailed above, I believe MARTINEZ used the same fraudulent identity of K.B. to apply for and receive SNAP benefits. The counterfeit Massachusetts driver's license bearing an image of a person who I believe to be MARTINEZ used in the vehicle fraud appears below.



83. In May 2024, Greenwood Credit Union also reported an additional fraud committed by a subject I believe to be MARTINEZ to the West Warwick Police Department. On January 25, 2024, a subject, who I believe to be MARTINEZ, used a counterfeit Rhode Island driver's license in the identity of J.J. to obtain a 2021 Can-Am F3MA motorcycle from MOMS Foxboro car dealer in Foxborough, Massachusetts by obtaining a line of credit using stolen identity information and leaving the dealership with the vehicle. Subsequent investigation by the Foxborough Police Department determined that MARTINEZ committed the fraud which resulted up to a loss of \$8,965.62 to Greenwood Credit Union.

84. As detailed above, I believe MARTINEZ used the same stolen identity of J.J. to apply for and receive SNAP benefits. The counterfeit Rhode Island driver's license bearing an image of a person who I believe to be MARTINEZ used in the vehicle fraud, which I believe is the same license MARTINEZ presented to me during the previously detailed undercover interaction, appears below.



Bank Fraud Investigation

85. In July 2024, the Greenwood Credit Union in Warwick, Rhode Island reported a check fraud incident to the Warwick Police Department. In March 2024, MARTINEZ used his true name, date of birth, and SSN to open a personal checking account and a business checking account in the name of "Maroon Express."

86. The Warwick Police Department investigation determined MARTINEZ deposited apparent altered or counterfeit checks in his bank accounts on various occasions, as detailed below.

87. In April 2024, a \$3,581.00 U.S. Treasury check altered to be payable to “Reynaldo Martinez” was deposited into the personal checking account of MARTINEZ.

88. In May 2024, a \$2,007.00 U.S. Treasury check altered to be payable to Maroon Express was deposited into the business checking account of Martinez.

89. In July 2024, a \$13,287.00 stolen business check altered to be payable to Maroon Express was deposited into the business checking account of Martinez.

90. In May 2024, RODRIGUEZ used her true name, date of birth, and SSN to open a personal checking account and savings account. The Warwick Police Department investigation determined RODRIGUEZ deposited altered checks in her bank accounts on various occasions, as detailed below.

91. In May 2024, a \$4,582.00 U.S. Treasury check altered to be payable to “Yanaiza Rodriguez” was deposited into the personal checking account of RODRIGUEZ.

92. In May 2024, a \$3,488.00 U.S. Treasury check altered to be payable to “Yanaiza Rodriguez” was deposited into the personal savings account of RODRIGUEZ.

93. The Warwick Police Department report indicated that surveillance footage shows MARTINEZ operated the SUBJECT VEHICLE to drive RODRIGUEZ to the Greenwood Credit Union to make cash withdrawals in May 2024 after the fraudulent checks cleared.

94. In August 2024, The Warwick Police Department obtained arrest warrants for MARTINEZ and RODRIGUEZ for state offenses related to the bank fraud for this conduct.

95. On October 28, 2024, the Pawtucket Police Department conducted a traffic stop on the SUBJECT VEHICLE for traffic violations. MARTINEZ was the operator of the SUBJECT VEHICLE with RODRIGUEZ as the passenger; both were arrested based on the Warwick Police Department arrest warrants.

96. According to records I reviewed from the U.S. Department of the Treasury, I believe MARTINEZ fraudulently negotiated five U.S. Treasury checks totaling \$49,957.00 in his own name and a likely fictitious business name into banking institutions, inclusive of the checks referenced above.

Subsequent Investigation

97. On November 5, 2024, U.S. District Court Magistrate Judge Lincoln D. Almond issued a tracking warrant authorizing federal agents to install and use a tracking device to monitor the location of the SUBJECT VEHICLE. On November 6, 2024, I covertly installed the tracking device on the SUBJECT VEHICLE at the SUBJECT PREMISES and subsequently monitored the location of tracking device, as authorized by the tracking warrant.

98. MARTINEZ was scheduled to appear before U.S. District Court Magistrate Judge Lincoln D. Almond on November 8, 2024, at 2:00 pm for a new supervised release violation as a result of his arrest in the Warwick Police Department investigation referenced previously.

99. Prior to appearing in U.S. District Court on November 8, 2024, MARTINEZ cashed an altered U.S. Treasury check in the name of another person in the amount of \$1,784.44 at approximately 10:33 am at Walmart in North Kingstown, Rhode Island.

100. MARTINEZ appeared before U.S. District Court Magistrate Judge Lincoln D. Almond on November 8, 2024, at 2:00 pm for a new supervised release violation. The government did not request the detention of MARTINEZ and he was not taken into custody at the hearing.

101. Following his appearance in U.S. District Court on November 8, 2024, MARTINEZ cashed a suspected altered U.S. Treasury in the name of another person in the amount of \$1,689.57 at approximately 3:48 pm at Walmart in North Attleboro, Massachusetts wearing the same clothes

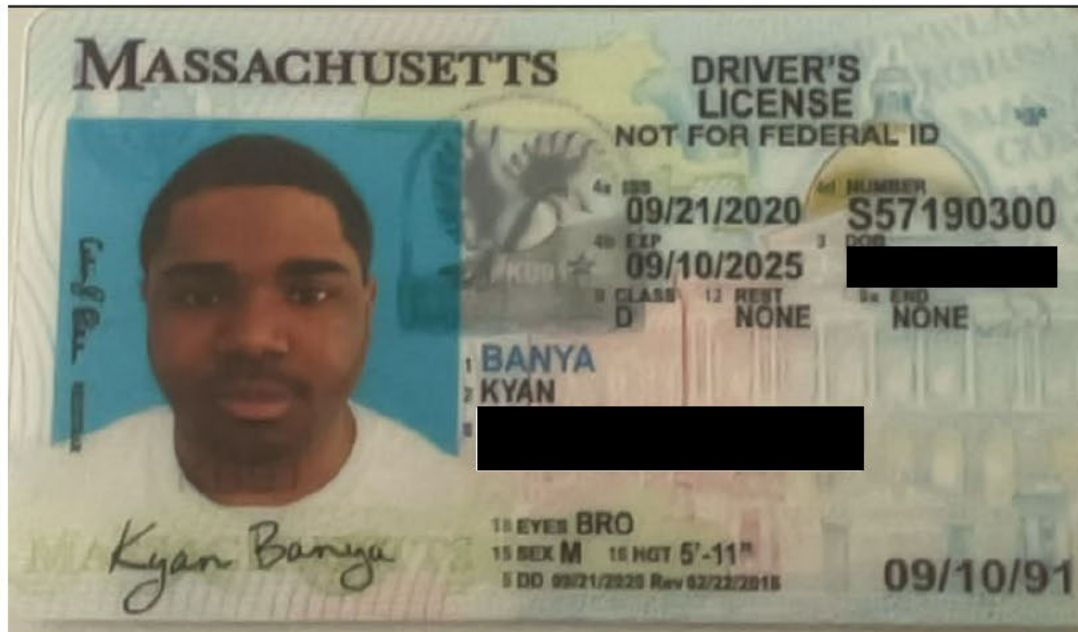
as he wore at court, as pictured below. MARTINEZ used the SUBJECT VEHICLE to drive to and from Walmart in North Smithfield, Rhode Island.



102. Following his appearance in U.S. District Court on November 8, 2024, MARTINEZ cashed a suspected altered U.S. Treasury in the name of another person in the amount of \$1,625.32 at approximately 7:59 pm at Walmart in North Smithfield, Rhode Island.

103. On November 8, 2024, MARTINEZ also purchased or attempted to purchase furniture from Raymour & Flanigan Furniture in North Attleborough, Massachusetts using his name to have furniture delivered to the SUBJECT PREMISES. MARTINEZ previously attempted to purchase furniture from Raymour & Flanigan Furniture using the identity of K.B. on three occasions as recently as November 6, 2024. Business records from Raymour & Flanigan Furniture

for the transaction(s) in the identity of K.B. include the below counterfeit Massachusetts driver's license bearing an image of MARTINEZ.



104. On November 13, 2024, MARTINEZ cashed a suspected altered U.S. Treasury check in the name of another person in the amount of \$1,300.00 at approximately 1:40 pm at Walmart in Northborough, Massachusetts.

105. Since the installation of the tracking device, federal agents and corporate loss prevention investigators documented MARTINEZ successfully cashing checks at multiple Walmart locations throughout Rhode Island and Massachusetts on at least 20 occasions, using different identities and identity documents on each occurrence. Walmart check transaction records documented the driver's license numbers of the Rhode Island and Connecticut driver's licenses presented by MARTINEZ to cashiers in order to cash the checks. I believe all twenty of the driver's licenses MARTINEZ provided to cash the checks to be fraudulent based on the driver's license numbers associated with the documents not being associated with any issued driver's license in

state databases. Additionally, there were believed to be at least 11 unsuccessful attempts by MARTINEZ to cash U.S. Treasury checks at Walmart locations during the same time period. The government is awaiting additional information from Walmart and the U.S. Treasury to be able to determine the legitimacy of the successfully cashed checks associated with MARTINEZ.

106. On October 31, 2024, Postal Inspector Cory McManus initiated a retroactive mail cover² related to USPS mailings going to the SUBJECT PREMISES. That mail cover captured mail images between October 2, 2024 and October 31, 2024. During this period, the mail cover included the following mail images:

- a. On October 2, 2024, a Navy Federal Credit Union statement addressed to RODRIGUEZ at the SUBJECT PREMISES.
- b. On October 7, 2024, a T-Mobile statement addressed to RODRIGUEZ at the SUBJECT PREMISES.
- c. On October 17, 2024, a USPS Priority package³ addressed to MARTINEZ at the SUBJECT PREMISES.

SUBJECT PREMISES

107. According to the Accurant database, the SUBJECT PREMISES is the residential address for MARTINEZ and the identity of K.B. based on a query in October 2024. I believe the association of K.B. to the SUBJECT PREMISES resulted from the fraudulent use of the identity

² A mail cover is an investigative tool utilized by the USPIS to gather information related to letters and parcels going to a specific address.

³ USPS Priority package from Shevan McDonald, wife of Jason McDonald, who was a co-conspirator of MARTINEZ in prior federal investigation in 2017 (<https://www.justice.gov/usao-ri/pr/13-million-fraud-ringleader-sentenced-federal-prison>)

by MARTINEZ who lives at the SUBJECT PREMISES. On November 5, 2024, November 6, 2024, and November 10, 2024, I observed the SUBJECT VEHICLE, which is leased to MARTINEZ, parked at the SUBJECT PREMISES. As of November 2024, MARTINEZ subscribes to internet service at the SUBJECT PREMISES on an account associated with MARTINEZ PHONE 2 and an email address associated his identity. I observed MARTINEZ at the SUBJECT PREMISES on November 10, 2024.

108. RODRIGUEZ provided the SUBJECT PREMISES as her address to the Pawtucket Police Department during her arrest on October 28, 2024. I observed RODRIGUEZ at the SUBJECT PREMISES on November 5, 2024 and November 10, 2024.

109. I believe evidence of the SUBJECT OFFENSES will be found at the SUBJECTS PREMISES. The evidence sought by the government, includes, among other things, records, documents, and digital evidence, related to the continuous and ongoing fraudulent activity of MARTINEZ and RODRIGUEZ.⁴

110. Based on my training and experience in similar investigations, individuals committing the SUBJECT OFFENSES often use their residences to store counterfeit documents, records, ledgers, currency, and other records which constitute evidence of these offenses. In identity fraud cases involving many victim identities used in the offense, such as this case, individuals committing the fraud often create ledgers or other written means to document and organize the scheme to include EBT cards and their associated dollar amounts and PINs.

⁴ See *United States v. Mitten*, 592 F.3d 767, 775 (7th Cir.2010) (“It is well established that the passage of time is less critical when the affidavit refers to facts that indicate ongoing continuous criminal activity.” (internal quotation marks omitted)); see also *United States v. Floyd*, 740 F.3d 22, 34 (1st Cir.2014) (“Business records, as a class, are repositories of historical facts and, therefore, are largely immune from claims of staleness.”).

111. The investigation documented the fraudulent acquisition and use of SNAP benefits by MARTINEZ and RODRIGUEZ. The purpose of SNAP is to purchase food using EBT cards. I know that food is very commonly stored in residences. Food products of various types can be stored for weeks or months prior to being consumed or resold. In cases food products are purchased in bulk from wholesale-type stores, larger quantities of food products are often possessed for longer time periods or are stored to be resold.

SUBJECT VEHICLE

112. According to the Rhode Island Division of Motor Vehicles, the SUBJECT VEHICLE is leased to MARTINEZ by Honda Lease Trust. The lease address (so called “garage address”) is an address previously associated with MARTINEZ and RODRIGUEZ in Pawtucket, Rhode Island, according to the Accurant database.

113. On October 18, 2024, MARTINEZ used the SUBJECT VEHICLE to transport counterfeit documents to and from a RI DHS office. On multiple occasions in August, September, and October 2024, MARTINEZ and RODRIGUEZ used a vehicle of the apparent same make, model, and color as the SUBJECT VEHICLE to drive to retail locations to use fraudulently obtained SNAP EBT cards.

114. On multiple occasions in August and September 2024, MARTINEZ and RODRIGUEZ used a vehicle of apparent same make, model, and color as the SUBJECT VEHICLE to transport items purchased with fraudulently obtained SNAP EBT cards from retail locations. On October 28, 2024, MARTINEZ (the driver) and RODRIGUEZ (the passenger) were occupants of the SUBJECT VEHICLE during a traffic stop in Pawtucket, Rhode Island. Based on tracking device location information, video surveillance footage, and records from Walmart and the U.S. Treasury, I believe MARTINEZ is actively using the SUBJECT VEHICLE to transport

altered and/or stolen checks and cash obtained from check fraud activity. On November 5, 2024, November 6, 2024, and November 10, 2024, I observed the SUBJECT VEHICLE at the SUBJECT PREMISES.

115. I believe evidence of the SUBJECT OFFENSES will be found within the SUBJECT VEHICLE. The SUBJECT VEHICLE is used by MARTINEZ and RODRIGUEZ to commit the SUBJECT OFFENSES by transporting counterfeit documents, fraudulently obtained EBT cards, and items purchased using fraudulently obtained EBT cards. Since the installation of the tracking device on November 6, 2024, the SUBJECT VEHICLE has travelled to over 15 different Walmart locations in Rhode Island, Massachusetts, and Connecticut to conduct over 30 successful or attempted check cashing incidents.

116. Based on my training and experience in similar investigations, I know individuals committing the SUBJECT OFFENSES use vehicles to travel to and from retail and banking locations, transport fraudulently obtained merchandise, and to meet with other individuals involved in criminal activity. I believe evidence of the SUBJECT OFFENSES such as counterfeit documents, receipts from retail and banking businesses, and fraudulently obtained merchandise are often found within vehicles used in the commission of the SUBJECT OFFENSES.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

117. There is probable cause to believe that electronic devices were used to violate federal law, and that the devices and equipment will be found at the SUBJECT PREMISES, on the SUBJECT PERSONS, and in the SUBJECT VEHICLE.

118. From my training and experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions

by communicating about them through e-mail, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

119. Further, based on my training, experience, and information provided by other law enforcement officers, I know that many cellular phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

120. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

121. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

122. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

123. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

124. Wholly apart from user generated files, computer storage media in particular, computers’ internal hard drives contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

125. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

126. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

127. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence

relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

128. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

129. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

130. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

131. Based on my knowledge, training, and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

132. The volume of evidence that storage media, such as hard disks, flash drives, CDs, and DVDs, can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

133. Technical requirements analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system

and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

134. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

135. The SUBJECT PREMISES, SUBJECT PERSONS, and SUBJECT VEHICLE may contain or possess computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

136. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with the offenses described herein. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

137. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement agents may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

BIOMETRIC ACCESS TO DEVICES

138. This warrant permits law enforcement to compel MARTINEZ and RODRIGUEZ to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

139. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

140. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch

ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

141. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes, and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

142. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

143. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to

unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

144. As discussed in this Affidavit, I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

145. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

146. Due to the foregoing, if law enforcement personnel encounter any devices for which they have a reasonable belief belong to MARTINEZ or RODRIGUEZ that are subject to seizure

pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of MARTINEZ and RODRIGUEZ to the fingerprint scanner of the devices found at the premises; (2) hold the devices found at the premises in front of the face of MARTINEZ and RODRIGUEZ and activate the facial recognition feature; and/or (3) hold the devices found at the premises in front of the face of MARTINEZ and RODRIGUEZ and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that MARTINEZ or RODRIGUEZ state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel MARTINEZ or RODRIGUEZ to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

147. Based on the forgoing, I respectfully request that the Court issue the proposed search warrants. I believe probable cause exists to show MARTINEZ and RODRIGUEZ have violated the federal criminal statutes cited herein, and that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES, more fully described in Attachment B, are located at the SUBJECT PREMISES, in the SUBJECT VEHICLE, and on the SUBJECT PERSONS, more fully described in Attachments A1-A4. I respectfully request that the Court issue the requested warrants authorizing the search of the SUBJECT PREMISES, SUBJECT PERSONS, and SUBJECT

VEHICLE and the seizure therefrom of the evidence, fruits, and instrumentalities described in Attachment B.

148. I respectfully request permission to obtain the assistance of other federal, state, and/or local law enforcement authorities, including an electronics detection canine, to aid in the execution of the proposed search warrants.

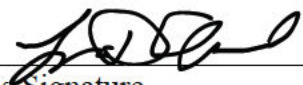
Respectfully submitted,


Special Agent Kyle Bishop
Office of Inspector General
United States Department of Agriculture

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1. by: **Telephone** (specify reliable electronic means)

Date **November 18, 2024**

Providence RI
City and State



Judge's Signature
Lincoln D Almond USMJ
Printed Name and Title

ATTACHMENT A-1
Property to be Searched

The SUBJECT PREMISES of [REDACTED] including the entire apartment, basement, attic, and common areas, is particularly described as the northernmost apartment within a three-unit residential building with blue/grey siding, white trim, and a white front door. The number “1” appears on a black mailbox on the front entry stairs leading to the front door.

Photographs of the SUBJECT PREMISES, with the front and rear entry doors identified with red ovals, appear below.



Source: Agent Surveillance (11/10/2024)



Source: Agent Surveillance (11/5/2024)

ATTACHMENT A-2
Person to be Searched

The person of Reynaldo Martinez described as an approximately 32-year-old male adult with dark eyes and approximately 5'9" in height.

Photographs of MARTINEZ appear below.

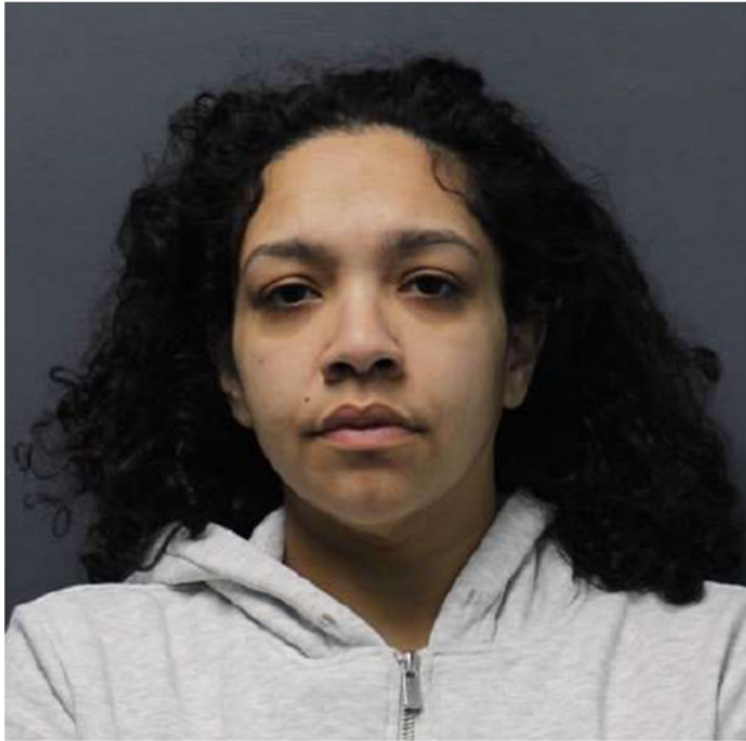


Source: Joint Automated Booking System (11/8/2024)

ATTACHMENT A-3
Person to be Searched

The person of Yanaiza Rodriguez described as an approximately 31-year-old female adult with dark eyes and approximately 5'2" in height.

A photograph of RODRIGUEZ appears below.



Source: Pawtucket Police Department (4/21/2024)

ATTACHMENT A-4
Vehicle to Be Searched

The SUBJECT VEHICLE is particularly described as a grey 2024 Acura MDX sport utility vehicle bearing Rhode Island passenger registration plate number 1SP242 with vehicle identification number 5J8YE1H42RL015565 which is regularly operated by MARTINEZ and RODRIGUEZ in the District of Rhode Island.

A photograph of the SUBJECT VEHICLE at the SUBJECT PREMISES appears below.



Source: Agent Surveillance (11/5/2024)

ATTACHMENT B
Particular Things to be Seized

All evidence, instrumentalities, fruits or contraband, in whatever form they are found, relating to violations of the SUBJECT OFFENSES, including but not limited to the following:

1. All electronic devices, computers, smart phones, and cellular telephones capable of internet connectivity or data storage.
2. All counterfeit, forged, and/or altered documents, records, and identification.
3. Indicia of occupancy including but not limited to mail or documents bearing the names of the occupants of the residence and vehicle being searched.
4. Any and all documents, records, and items relating to SNAP fraud, aggravated identity theft, and wire fraud, including, but not limited to, currency, treasury checks, cashier's checks, money orders, wire transfer records, bank records, ledgers, cash receipts journals, cash disbursement journals, cash register records, notes, SNAP EBT or WIC cards or coupons, EBT terminals, EBT keypads, and EBT customer lists.
5. Any and all documents related to identity information containing names, dates of birth, SSNs, and other personal identifiable information.
6. Any and all documents relating to transferring or secreting of money.
7. Any and all forms of communication and/or correspondence, including, but not limited to, memoranda, handwritten notes, letters, cellular telephones, facsimile, and email containing identity or financial information and/or between or involving the locations and/or individuals discussed within this affidavit.
8. Security cameras and video recording devices.
9. Authentic and counterfeit photographic identification of all types including driver's licenses, identification cards, and passports.

10. Supplies and materials used in the creation or alteration of identity documents including but not limited to scanners, printers, office supplies, watermarks, dies, presses, plates, tools, solvents, solutions, chemicals, lamination, mediums, seals, and related equipment.
11. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash drives, compact disks, and other magnetic or optical media.

- a. Computers, phones, electronic media storage devices used to process or store electronic media related to applications for SNAP benefits.
- b. Telephones capable of calling state or federal agencies that administer the SNAP or private entities who facilitate the SNAP.
- c. Documents containing personal identifying information.
- d. Mail or other correspondence to/from state and federal agencies that administer the SNAP or private entities who facilitate the SNAP.
- e. SNAP EBT and/or other financial transaction cards.
- f. Financial transaction card numbers.
- g. Applications for SNAP benefits.
- h. Applications for retailer participation in the SNAP.
- i. Point of Sale (POS) terminals.